S-125
ANNEX G
ITEM 1 of 2

TOP SECRET "U" 1. TICOM I/-57

Enciphering Devices worked on

by Dr. LIEBKNECHT at Wa Pruef 7.

Attached is a note on the personal data of Dr. Werner LIEBKNECHT of HWA Wa Pruef 7 and a translation by Lieuts. Howard and Tompkins USNR of a report by LIEBKNECHT of his work on German secret telegraphy and telephony devices.

TICOM
2nd Aug. 1945

No. of pages 15
Copy No. 28

Distribution:

British
1 Director
2 D.D.3
3 D.D.4
4 D.D.(N.S.)
5. D.D.(M.W.)
6 D.D.(A.S.)
7-8 A.D.(C.C.R.)(2)
9 Col. Leathem

U.S.
25-26 OP20-G(2)(via Lt. Pendergrass)
27 G-2(via Lt.Col. Hilles)
28-29 S.S.A.(2)(via Major Seaman)
30 Director, S.I.D. USFET (via Lt.Col. Johnson)

TICOM
10 Chairman
11-12 S.A.C.(2)
13 Cdr. Bacon
14 Cdr. MacKenzie
15 Cdr. Tandy
16 Lt.Col. Johnson
17 Major Seaman
18 Lt. Eachus
19 Lt. Vance
20 Capt. Cowan
21 Lt. Fehl
22-23 Ticom files(2)
24 Lt.Cdr. Manson

Additional
31 D.D.S.D.(Y) Admiralty
32 D.D.Y. War Office
33 D.D.I.4. Air Ministry
34 Mr. Twinn
35 Major Morgan
36 Dr. Turing

17 July 1945

PERSONAL DATA

DR. OF ENGINEERING WERNER LIEBKNECHT

(Only from memory)

1. Born 1 June 1905 at Waltershausen/Thuer

2. 1911-1916 Volksschule at Sonneberg/Thuer, parents' home

3. 1916-1925 Oberrealschule at Sonneberg/Thuer

4. 1925-1931 Study
   1925-1927 Technical High School/Muenchen "Electrical Engineering"
   1927-1931 Technical High School/Berlin "Communications Engineering". Graduating with diploma, Dipl.-Ing.

5. Feb. 1932 - May 1932 Heinrich-Hertz-Institut für Swingungsforschung/Berlin, Broadcast Receiver Section.

6. June 1932 - Dec. 1936 Technical High School/Berlin, Assistent am Lehrstuhl for distant reporting technique, wire communications technique. In may 1936, Dr.-Engineering.

7. Jan. 1937 - 9 April 1945 Communications Section HWA Berlin (Wapruef 7), civil servant
   A) 1 Jan. 1937 - 1 May 1942 in Group Wapruef 7/II
   Wire Communications Technique
   Field of work

Speech	Telegraphy
Work on technical questions of speech scrambling for the Army	Work on technical questions of teletype encoding, SZ 40, SZ 42 for the Army.

   B) 1 May 1942 - 9 April 1945 in Group Wapruef 7/III
   Wireless Communications Technique
   AA) 1 April 1942 - 1 July 1943, field of work the same as in Wapruef 7/II
   BB) 1 July 1943 - 9 April 1945, field of work expanded to include hand encoding devices, before then the work of Wapruef 7/IV, Dr. Pupp

SUMMARY OF TECHNICAL ACTIVITIES:

1. Main field of work, technical work on speech scrambling.

2. In the field of telegraphy, work on the automatic encoding devices SZ (Schluesselzusatz) 40 and SZ 42

3. In the field of hand encoding equipment, no properly technical activity, only the direction of current developments.

19 July 1945

SUMMARY OF THE ENCIPHERING DEVICES WHICH THE UNDERSIGNED (LIEBKNECHT) HAS WORKED WITH IN HWA

(NB--This paper represents a free translation by Lieuts. C.B. Tompkins and J.H.Howard of a report written by Werner Liebknecht while he was being held at Revin, France)

I. DEVICES FOR TELEGRAPHY

A. Device for Automatic Enciphering.

0. See Insert No. 1 for description of "Typenbildverschlüsselung".

1. The SZ (Schluesselzusatz) was used in two different designs for the automatic encipherment of start-stop teletype: The SZ 40 and the SZ 42. Both devices were used as attachments to ordinary teletype machines so that the ordinary machine was connected in series electrically with the SZ. The ordinary teletype machine is in no way altered mechanically.

The working principle can be described as follows: the five element signals emitted by the ordinary teletype are stored in the receiving section of the SZ. This storage takes place in a mechanical system such as is used in Germany in the teletype machine produced by C. Lorenz A.G. The SZ starts on the arrival of the first teletype impulse, which causes the cipher wheels to turn. While the first letter is entering the machine it causes the emission of the first encoded impulses. The encoding takes place therefore in the SZ from pulse to pulse in the order of 1-2-3-4-5 etc. In the receiver, the encoded letters are similiarly stored in an SZ. Again a mechanical receiving system is used for this storage. Each SZ contains therefore two mechanical accumulators, one for the reception of plain teletype text from the ordinary machine and one for the reception of encoded text.

There is only one set of cipher wheels for the two systems. The connection of the cipher wheels to the receiving system depends on what receiving system first trips. The tripping of one of the receiving systems automatically blocks the other.

Both SZ's were equipped with wheels with variable lugs. It is possible therefore to set a number of lugs on each wheel according to its divisions without exchanging wheels.

The SZ-40. The "40" denotes the year in which the SZ-40 was built. It works with 10 wheels. The device was produced only in small numbers (about 100) by the Ingenieurbuero Zehlendorf of the firm C. Lorenz A.G., Berlin. Since the tests of Chiffrierstelle OKW/Chi quickly showed the machine to be inadequate, a new development had to be started.

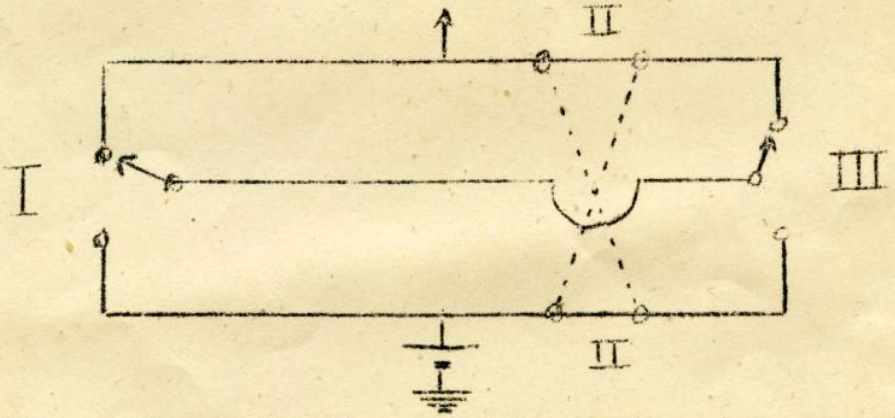
The SZ-42. As directed by OKW/Chi (Reg-Rat Dr. Huettenheim, Dr. Stein) the device had to be reconstructed as follows: the machine as compared with SZ-40 had to have two additional cipher wheels making therefore a total of 12. The 12 motor wheels (Einstellraeder) had the following function from left to right. The first five wheels are called "Spring-Caesar". (NB. Liebknecht says the term Caesar is used by the Germans for items associated with encipherment since Caesar was one of the first to use enciphered communications. The term Spring denotes irregular stepping). They are driven irregularly. The irregular motion is achieved through the stepwise stopping of the whole group of 5 wheels. The progress of the stepwise stopping is determined by wheels 6 and 7.

The wheels 6 and 7 are called "Vorgelege" (control) for the "Spring-Caesar" wheels. Wheel 7 steps Wheel 6 in accordance with the lug settings chosen for it. Wheel 6 determines in accordance with its lug settings and its motion the stopping of the Spring-Caesar group 1-5.

Wheels 8 through 12 are moved regularly and shift one another only in accordance with their prime number divisions. They are called "Spalten-Caesar". (NB. The term Spalten denotes a one-to-one correspondence between the controlling and controlled wheels as contrasted to a shifting around between the two according to Liebknecht). A prime number of divisions were chosen for all wheels 1 to 12.

The fundamental encoding principle: the encoding of the separate impulses one after another was still used.

The following diagram illustrates the method of encoding the separate impulses.



The question whether the encoded impulse is mark or space is determined by three groups of switches:

Switch I is set by the plain text to be encoded in the receiving collector.

Switch II is set by a wheel of the Spring Caesar, that is ZRL (NB-to be explained below) to activate Switch I.

Switch III is activated by a wheel of the Spalten-Caesar which is ZRL to Switches I and II.

The term ZRL (Zeitlich Rightig Liegen) means the following: When the impulse in its coded value is introduced, all switches which determine this impulse must be well seated in place; that is, they must have been in position with a safety factor in time, and ought to be reset only after the emission of the impulse. Only this way can troubles with contact bounce be prevented. The contact times of the various switches are "ZRL".

Switch Group II is shown only symbolically in the diagram. Its function is to reflect the workings of Switch Group III. In the position (A) the solid lines apply and in position (B) the dashed lines apply.

PLAIN TEXT FUNCTION (KT)

The KT function was to increase the security of the device through the lengthening of the running period of the Spring Caesar. This function was brought about as follows: if the incoming 5 element teletype signal has a mark in the 3rd or 5th impulse (L. was not sure which) a stop command for the Spring Caesar for the next letter is canceled. The whole Spring Caesar Group is hereby controlled. The KT could be bypassed. It can be worked with the KT either on or off.

In operation the KT function becomes noticeably unpleasant. In the off position, a failure of one impulse causes only one garble in the receiving teletypewriter, whereas in the on position a failure will cause a failure throughout the rest of the message. The operation must therefore be interrupted after only one garble and the enciphering apparatus be reset.

SZ was used both on land lines and on radio circuits, mostly in connection with the well-known "WTZ" apparatus on radio; whereby in each direction two carrier frequencies are used for each teletypewriter. The SZ weight is 110 to 125 pounds. Because of its strong construction, good continuous service is obtained.

2. Teletype encoding with synchronization (Gleichlauf)

During operation with automatic stepwise working teletype scramblers, frequent failure through false impulses arises causing the equipment to get out of synchronization. The equipment must then be reset very frequently. The same applies for fading. The problem comes up then of producing a scheme whose synchronism is independent of false impulses transmitted over the connecting channel.

The question was solved in the Feuerstein Lab. in Ebermannstadt/ Oberfrankonia working in conjunction with me. The result was called "Schluesselfernschreiberanlage mit Gleichlauf". Gleichlauf works on the following principle.

The transmitting--and the receiving encoding--apparatus will start in synchronism from a signal from the sending part. After the start the encoding devices run on controlled by self-contained crystal regulating apparatus, and are therefore free of any deviation from synchronization caused by false impulses over the connecting path.

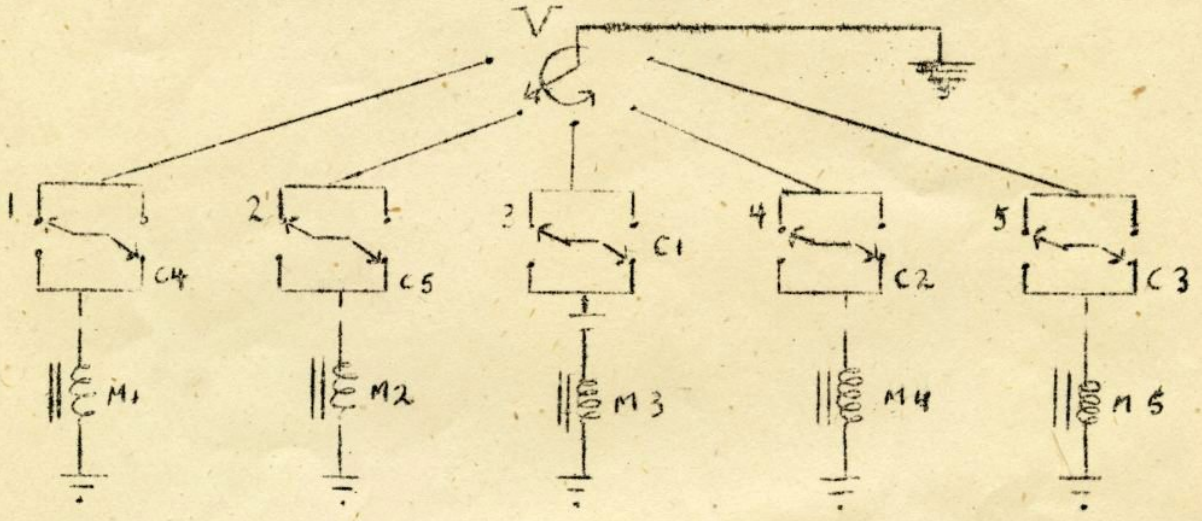
The encoding devices run all the time even when there is no traffic. The Gleichlauf was equipped for 4-wire traffic and therefore worked with 4 encoding devices. The two traffic directions must be started separately.

The output of the system was equipped for 7 or $7\frac{1}{2}$ element teletype code, so that for each day a maximum of about 500,000 teletype signals can be sent.

Since Gleichlauf works with continuously-operating codeing devices, pure key is sent during no traffic periods, and so OKW/Chi (Dr. Huettenheim, Dr. Stein) directed that the SZ42 be improved for use with the Gleichlauf. The remaining regularly stepping cipher wheels 8-12 in SZ42 should be changed to irregularly stepping wheels for increasing the security.

The development of the new SZ42 was to be carried out in the engineering bureau of C. Lorenz at Muehlhausen in Thueringen (moved from Berlin) but it could not be completed. The first model of the improved SZ42 (for Gleichlauf) still had mechanical faults and remained in Muehlhausen.

For the irregular stepping operation of the Spalten-Caesar wheels of the SZ42, the following switching principle was used: the operation was supposed to take place stepwise through impulse pawls.



M1 to M5 are magnets to activate the pawls, the stepping switch, and the stepwise further switching of the Spalten Caesar wheels. C1 to C5 are contacts which are activated by the corresponding Spalten Caesar. The contacts 1-5 can for example be activated by the wheels 1-5 of the Spring Caesar. Fundamentally, it is a result of this operation that the magnets M1-M5 influence themselves cyclically in their switching--M1 and C1 control M3, M2 through C2 controls M4, etc. The shifting of the contacts for example from C1 (M1) to the control circuit of M3 achieves safe switching. Through the distributor switch V, which periodically switches in the magnet circuits M1 to M5, in the sequence 1,2,3,4,5 it is achieved that during a five element signal each magnet is only propositioned once.

The new SZ42 was to get only 10, lug wheels, dispensing with wheels 6 and 7, the 2 so-called control wheels for the Spring Caesar 1-5. The operation of the Spring Caesar was to depend upon the by now irregularly driven Spalten Caesar wheels, for example, by a contact M2-C2. In the switching principle diagram, for stepwise control one can consider all possible switch positions and he will find the so-called dead position--a combination of switchings wherein none of the 10 coding wheels can move--since M1 to M5 will remain without current despite continuous rotation of the Distributor Switch V.

In order to prevent complete stopping of all wheels, and thereby the stopping of the cipher device, whereby all plain text sent through the device would result in monoalphabetic substitution, a counting mechanism was provided. This counting device had the task of counting, depending on the setting, two or three stationary steps and then, by removing the blocking of the Spring Caesar, bring the entire apparatus back into running. The use of a possible second counter which was to be provided for mechanical safety had not yet been incorporated in the diagram. This incorporation does not influence the principle of the machine.

The new SZ42 developed according to the above principles was at first to be equipped only for SFG (Gleichlauf), however it was later to be used for automatic cipher operation without Gleichlauf (i.e. for ordinary start-stop teletype traffic).

Complete switch-production-plans for the Gleichlauf are now to be found in the factory in the Feuerstein Lab at Ebermannstadt/Ofr. or its offshoot in Kirchental near St. Martin over Lofer/Austria.

3. Gleichlauf by F.A.--C.Lorenz, Muehlhausen/Thuer.

As a parallel development to that of the Feuerstein Lab. the engineering bureau of the Fa. C. Lorenz, Muehlhausen, had developed an experimental model of a syn. scheme. The equipment works in the main on the same principle as that of the Feuerstein Lab. and differed only in external construction. I am in doubt as to the continuation of the Lorenz model. The construction plans have been found by now in Muehlhausen. One part of the test equipment should be now in the Feuerstein Lab. The Lorenz equipment was to be tested in parallel with the Feuerstein equipment in the beginning of 1945.

4. Encoding Teletype Machine Type T52 (SFM T52)

The T52 is a combined encoding teletype machine consisting of a start-stop writer and an encoding attachment and was manufactured in Berlin by Siemens and Halska.

This encoding apparatus was not a product of HWA but was sponsored by the Navy -- Capt. Singer. Fundamentally the following can be said about this machine. The machine works with 10 cipher wheels which in the old models were driven uniformly. Later on irregular stepping was introduced for some of the wheels. The wheels have no variable lugs.

SFM T52 has been known in Models A through E. Further details can be obtained from the Mathematical Cipher Section of OKW, Dr. Huettenheim and Dr. Stein.

5. Encoding Teletyper T43 (See Insert No. 2 at back of report)

B. DEVICES FOR ENCODING BY HAND

1. The Enigma

The Enigma was the oldest, best known, and most used equipment. The equipment has been modified only in unessential ways during the last years. In regard to encipherment, the most remarkable change is called Lueckenfuellerwalze. On the rim of the normal Enigma drum there is only one carryover notch, by means of which the drum is advanced one step at a time. The Lueckenfuellerwalze (LFW) which was developed by the OKH Cipher Section working with OKW/Chi was so designed that an arbitrary number of carryover notches could be set at arbitrary points on each of the new LFW's.

The variable notches were designed in accordance with the variable lugs on the automatic cipher devices. There were no difficulties in construction. I do not know how far the LFW was actually put into use. The manufacturer in large numbers was just beginning.

The so called "Enigma-Uhr" was another attempt to improve the deciphering stability. The uhr was supposed to facilitate the otherwise complicated changing by hand of the plugboard, in order to accomplish quick cipher changes. The uhr was developed in many experimental models by the air forces and was said later to have been manufactured by them. I know nothing about exact constructional details. Mathematical researches in regard to encipherment on the uhr were carried out at first only by the air forces (Lt. Col. Schulze, Koethen) and later in conjunction with the OKH/Chi (Major Kempe) and OKW/Chi (Dr. Huettenhein). I do not know to what extent and whether the uhr was used.

2. Coding Equipment No. 39

From the numerous experiments the security of the Enigma, the fundamentals of the 39 came into being. On special request, the output per minute was to be increased to equal the normal start-stop teletype speed.

As indicated by the number "39", which was the year first set for its completion, experiments on such equipment have continued for many years. This delay was due in part to lack of clarity in the operational requirements, in part due to changes following mathematical researches, but in a large part to pure technical difficulties.

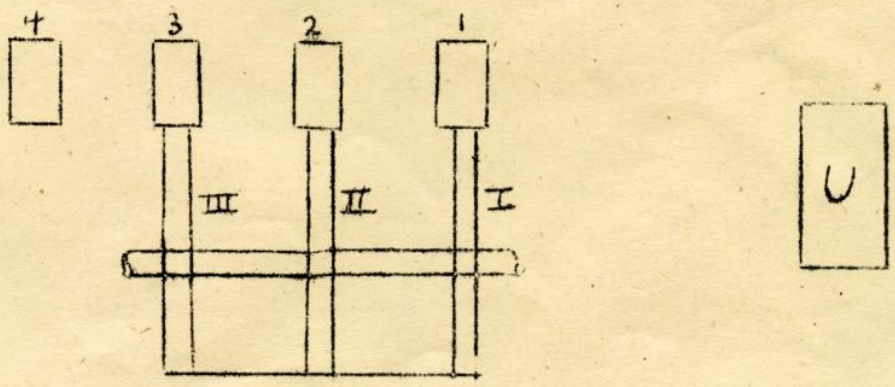
The 39 was developed in the Fa. Telefonbau und Normalzeit in Frankfurt-am-Main. The first experimental models were to be delivered in Feb. or March of 1945. Due to the development of the war, the equipments were not delivered. I know nothing concerning the whereabouts but perhaps the director of the T and N can give more details.

The 39 works on the Enigma principle -- i.e. it has cipher wheels with 26 passages and 26 sliding contacts. The many sliding contacts and the high output (7 letters per second) resulted in such a deterioration of the cipher wheels and sliding contacts that the life was low.

In order to attain a lifetime of 1 to $1\frac{1}{2}$ years of the cipher wheels, the maximum output had to be decreased--and it could not and must not be operated with automatic transmitters.

No. 39 was designed in detail as follows: in the space taken by the old Enigma was placed: a typewriter keyboard, 4 encoding wheels and 3 driving wheels, a driving motor for 12 to 220 volts, and a double printer. It printed the clear text and the cipher text separately on paper strips. In this manner mistakes in encoding could be easily detected.

The design with regard to encipherment is shown in the following diagram:



The wheels 1, 2, and 3 are driven the same as in the normal Enigma. Wheel 4 is not driven but is set by hand. The wheels I, II, and III represent a special drive the wheels 1, 2 and 3. I has 21, II has 23, and III has 25 teeth. The drive through the wheels I, II and III is superimposed on the normal drive of wheels 1, 2, and 3. (NB L. says the wheels I, II and III have choices of 21, 23, and 25 settable turnover lugs).

The Switch U replaces the plugboard in the normal Enigma. It can easily be removed and wired in a highly arbitrary way. The 39 was equipped with an attachment which permitted adjustment to print 3 or 5 letter groups. A separately developed power circuit permitted operations of the equipment from power mains.

2A. Schlüsselgerät 41.

The encoding device 41 was a hand encoding device developed by OKW/Chi working with Wa-Pruf 7/IV, Dr. Pupp. The device was arranged for purely mechanical operation by pressure for encoding and decoding. The machine was found to be faulty by OKW/Chi and was not adopted officially. About 1000 of a model with changed keyboard form (10 keys) was made by Wanderer/Chemnitz; this was a measure of expediency. The equipment was the "41Z". I know nothing concerning its adoption and further orders.

3. Encoding device "Schluesselkasten" (also called "Schieber")

The SK is a development of OKW/Chi (Dr. Huettenhain). The mechanical construction was at first taken over by T. and N. on Frankfort-am-Main. Later the development was transferred to the Wanderer Werks in Chemnitz.

The SK looked like a slide rule but was 2 to 3 times as wide. The operation of the SK was approximately as follows. The tongue of the instrument was shoved by hand to the right as far as it would go, thereby putting a spring inside the SK under tension. By means of pressure on a blocking notch on the top of the SK, one causes the sliding tongue to move back varying step lengths into the SK.

The control of the step lengths arises from 3 wheels with variable notches. On the sliding tongue and along side this tongue on the SK, the alphabet is entered in pencil by hand in scrambled order prescribed by the code book. The code book was not yet completed, however it was still being worked on by OKW/Chi and OKH/Chi (Dr. Huettenhain, Oberinsp Menzer.) The mechanical construction of the apparatus had to be changed many times during the course of experiments since the control of the stepping never worked well. The latest model of the equipment should have been finished in April by Wanderer/Chemnitz. However it was not delivered.

4. Encoding device "Schluesselscheibe"

Oberinsp Menzer designed this machine for agents. The machine was not to exceed in size a shoe polish can. The encoding principle was similar to that of the SK. The equipment of a rotatable inner disk and a stationary frame. The disk and frame had to be provided with scrambled alphabets similar to the SK. In operation the inner disk was rotated against the frame, and thereby in a manner similar to the SK put a spring under tension.

By means of pressure and a blocking notch, the disk is returned in various step lengths back toward its original position. In contrast to the SK, in this machine only control disks with fixed notches

were to be used. In the design three control wheels to be set from the outside were to be included. The number of notches was to be determined once and for all for each pair of devices (one for the agent and one for central office). For this, a hand punch was thought of for punching the notches. The devices were to be used only for line traffic.

These devices and their code books were only in the early stages on construction. There existed only an operating model without control of wheels. In how far Wanderer has completed plans for a satisfactory model is not known.

II DEVICES FOR TELEPHONY

The encoding of telephony represents essentially more complicated problems than the encoding of telegraphy. The tasks separated into two parts:

1. The encoded speech must be entirely unintelligible if heard through a normal phone.
2. The changing of the speech must take place with a sufficiently long period to meet all mathematical requirements for telegraphy devices.

The experiments of the undersigned lay mostly in the field of problem 1 above. The problems of part 2 could not be attacked since none of the known processes gave a satisfactory solution to part 1. If a process giving ununderstandable speech was arrived at, then unfortunately it always happened that the speech quality after unscrambling was no longer acceptable and the process of scrambling was therefore unacceptable. In connection with problem 2 above conversations with industry were carried on but no experiments were attempted. Speech scramoling experiments were conducted by several German firms during the years 1937 to 1940:

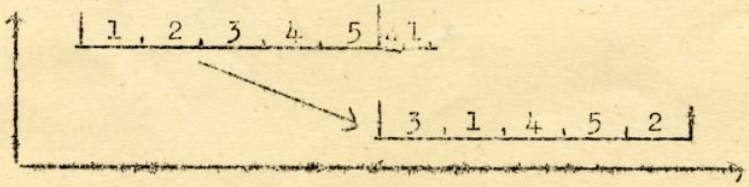
1. Siemens & Halske, Berlin
2. Deutsche Telefon und Kabelwerke, Berlin
3. Sueddeutsche Apparate Fabriken, Berlin
4. A.E.G., Berlin
5. Telefunken, Berlin
6. Dr. Vierling, Tech. Hochschule, Hanover
7. Fa. C. Lorenz A.G. Berlin/Muehlhausen/Thuer

Since, especially after 1940, the manpower shortage became more acute and the problems of speech scrambling were not always assigned a high priority, these firms had to cease their activity. In 1943 only Telefunken and Dr. Vierling worked on the problem. Dr. Vierling had meantime moved his shop from the school to Wennebortel, near Hanover, and was occupied with the planning of a new enterprise near Ebermannstadt/OFR, near Nuernburg. After 1944 only Dr. Vierling worked on the problem of speech scrambling after the completion of his new laboratory, named the Feuerstein Laboratory. Beginning in April 1945 some of the departments of the Feuerstein Laboratory concerned with the problem of speech scrambling and telegraphic encoding were moved to the south. Freilassing was the first stop. Since they could find no suitable quarters for the works here, they moved on to Salzburg. For reasons of better security against air attacks the works were once more moved to Kirchenthal near St. Martin, Ueber Lofer. Here at the end were the only parts for experiments on speech scrambling.

In detail, the following technical experiments were conducted.

1. The process of time scrambling (also called the Tigerstedt Process TDS

For the time scrambler the speech was stored usually on a magnetic ribbon. It was divided into a determined number of equal parts and was then transmitted in a different order. In principle the sequence 12345 was, for example, changed to 31452, or, as represented by the diagram



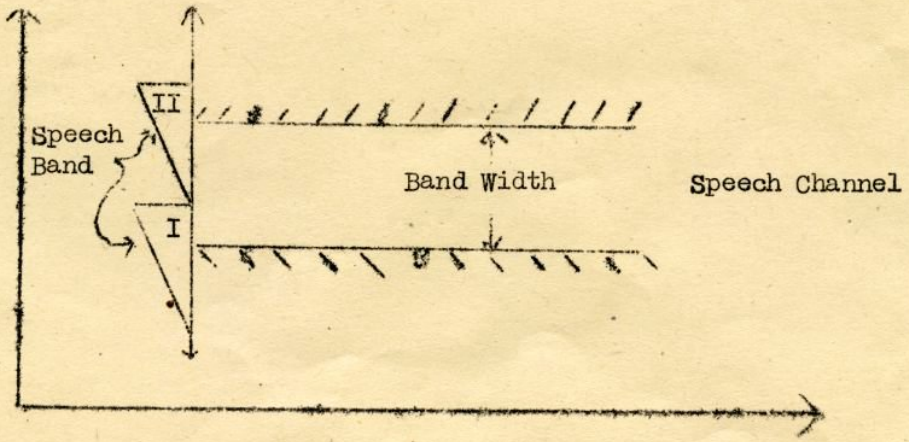
For the length of a siggle element 60 milliseconds was found to be the most favorable value. Experiments on the special processes of scrambling the elements were not undertaken, for the process when used to meet the general requirements prescribed gave no completely unintelligible speech. The process also was not acceptable because of the long storage time. The running time of the speech could be increased to unacceptable values without really attaining unintelligible speech.

Siemens, Berlin, some years ago brought out a further development of TS in which the following principle was applied. The speech was divided into three bands and each band separately scrambled. Despite the large bulk of this equipment (each station weighed about 2-3 zentner) this process did not deliver completely unintelligible speech. The device was never manufactured. 3-BAND TDS

Special difficulties arose with the experiments with the TS process and with all speech storing problems since the steel bands generally used rub and grate on the heads and then work sloppily. Experiments were undertaken to work with an air space between the head and the band. The experiments were undertaken at Lorenz, Muehlhausen and were just starting. A 0.5 mm air space could be bridged in the laboratory.

2. Process of frequency shifting (wobbling).

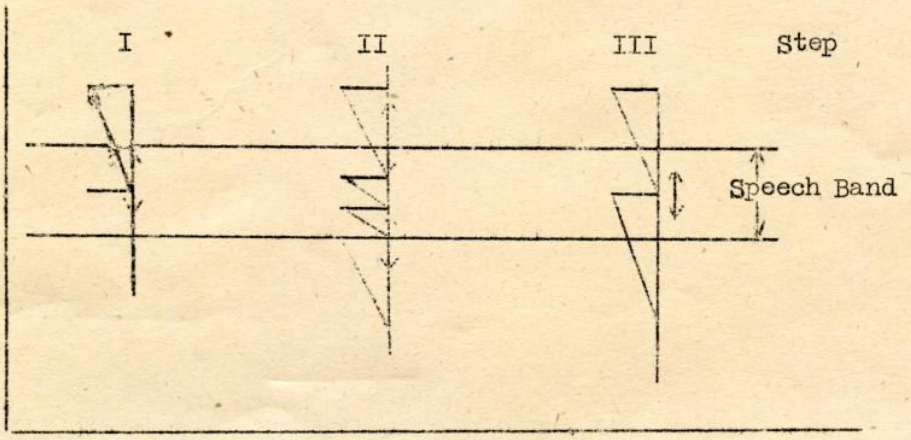
Wobbling works so that the speech is modulated on a carrier with this carrier periodically changing its value. The experiments centered basically around the so called ring wobbling. This works by transposition over the normal speech band of another band shifted one speech band width up. The two bands were modulated on one carrier and the carrier wobbled in front of a band filter, one speech band width wide. In principle the following diagrams represent the operation.



For wobbling the following average values were used: wobble frequency, 1/2 to 15 cycles; wobble center, 2,000 to 500 cycles (Wobbelhub).

A. Triple wobbling

Since the normal wobbling accomplishes no complete covering, that is completely unintelligible speech, the Fuerstein Laboratory in connection with OKW/Chi was developing a system which provided three complete wobble steps, in which the second step was divided into two smaller steps. The following scheme was used in principle.



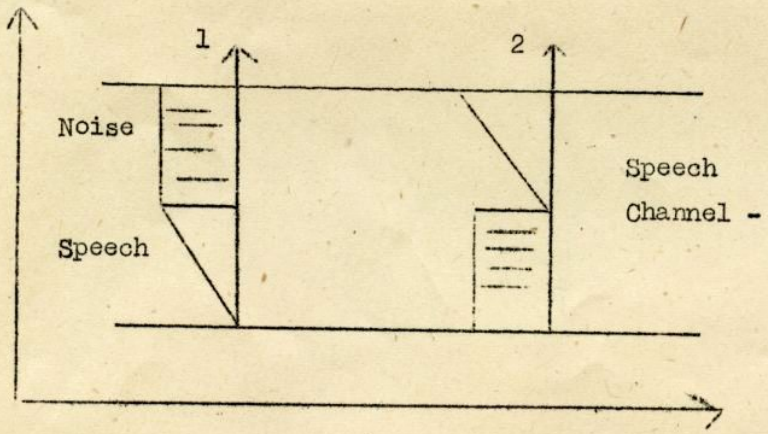
The wobbl ng was to be brought about in three steps through four separate wobble frequencies. The four wobble frequencies are to be shifted possibly through the use of an ordinary telegraphic enciphering equipment (SZ 42), whose mathematical security is already established.

Some experiments were made along these lines, but they were quickly seen to be impracticable because of their complexity. A project is still under way at LF (Feuerstein Laboratory), but it is also very complicated. Through this system, condensers were to be turned under the influence of teletype impulses from the SZ, and thus the wobbling is to be brought about. Until now the results from triple wobbling (formerly called WTV) have not been very satisfactory. The speech quality after dewobbling was very bad even when the same carrier was used for wobbling and de-wobbling. It is supposed that this bad result can be attributed to the auxiliary plug board. It can, however, also arise from the series switching involved in so many modulation steps. Numerous documents concerning the plugboard of the WTV are to be found either at LF or at its St. Martin branch.

B. Baustein.

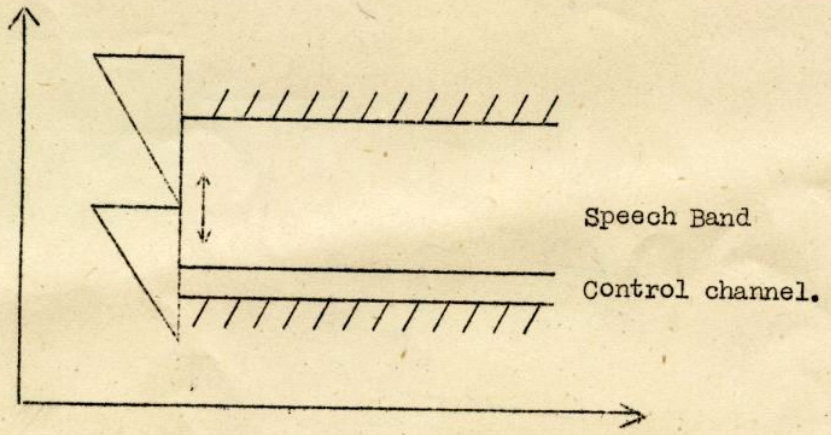
Since the experiments indicated that too much time was necessary to carry out the researches required to produce a secure machine, plans were developed for the independent construction of a machine which could be built quickly and which needed no settable key, but which was, in fact, better than the well known inverter. From these specifications LF made the two following developments: the Little Baustein and the Large Baustein.

The Little Baustein works on the following principle. 2 BAND SPEECH/NOISE ALTERNATION



A vacuum tube switches between a narrow speech band and a noise band so that in switching step 1 the noise is above and the speech below and in step 2 the positions are reversed. The switchings repeat periodically. The noise band carries over into the upper edge of the speech band. A sample of the machine is available in LF/St. Martin; the speech quality is at present not so good.

The Large Baustein utilizes the principle of ring wobbling.



As a special feature, the Large Baustein was provided with some autoencipherment. This was designed so that the wobble frequency was varied depending on the speech dynamics and was otherwise constant. This was to work with a known delay time.

The control impulses from the speech dynamics were delayed a period of 100 to 200 milliseconds and then used to control the wobble frequency. A kind of echo effect resulted that brought about a particularly good covering of the speech. The wobble frequency is transmitted in a special control channel.

The experiment resulted in such difficulties in control of the receiving equipment that the experiment up to the present has led to no conclusions. More detailed plans are at LF.

C. SYNTHETIC SPEECH.

Synthetic speech was developed at LF on the basis of American researches. Devices with 15 and with 8 channels were developed. Plans of the technical works can be found at LF.

The scrambling of channels for encipherment was soon found to be worthless, and it is a very problematical process to superimpose noise

voltages on the signal voltages in the various channels to attain secure encoding. Evidently the use of synthetic speech with triple wobbling gives the most promise of success. The question of speech quality should have special attention.

D. TIME WOBBLING.

In connection with the use of steel tape recorders with an air space, experiments were also conducted in which the head was moved periodically so that a kind of time wobbling was attained. These experiments did not progress beyond their initial stages. Further details can be obtained at C. Lorenz, Muehlhausen.

E. NOISE SUPERIMPOSITION

The method of noise superimposition requires that the noise bandwidth should be the same as that used for speech, resulting in a noise/signal ratio and that the combination is unintelligible. At the receiving end a noise exactly equal to that applied at the sending end in voltage and frequency and exactly 180 degrees out of phase so that the interference is compensated and clear speech remains.

This method has been used in Germany by C. Lorenz Berlin and Telefunken Berlin.

C. Lorenz Berlin 1937-1939 results of the experiments: the speech quality was very poor because of faulty compensation for the noise. The distortion during transmission over lines was too big.

Telefunken Berlin 1939-1943 Despite exhaustive experiments, workers under Dr. Kotowski concluded that it is impossible to compensate for the noise at the receiver end and that the speech quality is not acceptable. The at-that-time acting chief of Wa Pruef 7 assigned to Telefunken, however, in spite of these experimental results, the commission of setting up a complete radio link between Athens, Crete and Derna. Telefunken took over the complete commission, but mainly in its interests in "Friedensplane", to carry out field strength measurements in the UHF region. Experiments with noise superimposition are negative.

F. CHANNEL SWITCHING.

The Reichspost, Schbearbeiter Postrat Schmidt, had developed a method that employed two double lines to carry the speech. Through synchronous switching at the sending and receiving points the lines are interchanged arbitrarily. The equipment, then, split and then recombined the speech band. This is all I know about the device. Listening tests indicated that parts of the speech were understandable, that the method was therefore of only little value. I know nothing about the operation of, adoption of or orders for the device, for cooperation with the Reichspost was continually poor.

INSERT NUMBER ONE

(This and the following inserts were prepared by Liebknecht while at Ebermannstadt.)

Paragraph 1-A-O. TYPENBILDVERSCHLUSSELUNG (Teletypewriter Encoding)

The encoding of teletypewriter was the subject of researches by Dr. Hell, Berlin/Zehlendorf for several years from 1938 to about 1941. In spite of extensive experiments he was unable to make a machine supplying a high enough number of keys and thereby acceptable to OKW/Chi.

Dr. Hell had entirely given up his experiments by 1941. The "Bildverschlusselung" is an instrument very similiar to the typenbild-verschlusselung.

The only thing known about "BV" is that C. Lorenz Berlin Templehof about 1938 tried to achieve a kind of privacy in facsimile transmission by varying the timing number of their ordinary picture transmission apparatus. Lorenz gave up the experiments almost completely, for despite this encoding the pictures were easy to recognize.

INSERT NUMBER TWO

5. Teletype Encoding Machine T43

Obstlt. Schultze Koether developed for the Luftwaffe a device whose principle has long been known. The device was to apply punched paper tapes for encoding and was therefore only for two station traffic. For a line two completely equal punched five hole tapes would be provided, one for the sender and one for the receiver and they are advanced stepwise by writing on the machine.

The T43 is applied to a Siemens teletype machine on which is built a carriage for the tape. Each plain text character is mixed with a character of the punched encoded tape and then sent.

Siemens/ Berlin undertook the manufacture of the machine. I know nothing concerning further technical details of use or orders for the machine.